Background

If the user you have compromised has the role "Application Administrator" assigned to it that role can be used to manage Azure Applications. One such application is AzureAD - the application that administrer the AzureAD. A user with the role "Application Administrator" can add credentials to the AzureAD application. After that the user can impersonate the AzureAD application and then edit AzureAD users, and thereby escalate its privileges.

Pre-requisites

AzureAD user with the role "Application Administrator".

Risks

How to check for

How to exploit

Recommendation

Related Vulnerabilities

This finding should not be reported as the name of this issue, instead it should be reported as the vulnerabilities written below. The below written vulnerabilities map to the vulnerability-descriptions in that repo.

For example, if kerberoast, report as the following vulnerabilities if they are applicable:

- Weak password [ID of issue]
- Overpriviliged kerberoastable user [ID of issue]

References